White Paper

Navigating Privacy and Consent: A guide for digital health start ups

mohawk
IDEAWORKS
mHEALTH & eHEALTH DEVELOPMENT
AND INNOVATION CENTRE

In mid-December 2019, fifteen million Canadians woke up to the news that their personal data may have been breached. LifeLabs had been hacked. The company and its three subsidiaries perform 112 million diagnostic, monitoring, genetic and disease prevention tests in the country every year, making them a significant target for privacy breaches.

Access to digital healthcare services provides unprecedented levels of opportunity to prevent illness and improve health outcomes. Threats to digital privacy accompany each of these opportunities.

mHealth & eHealth Development and Innovation Centre (MEDIC)

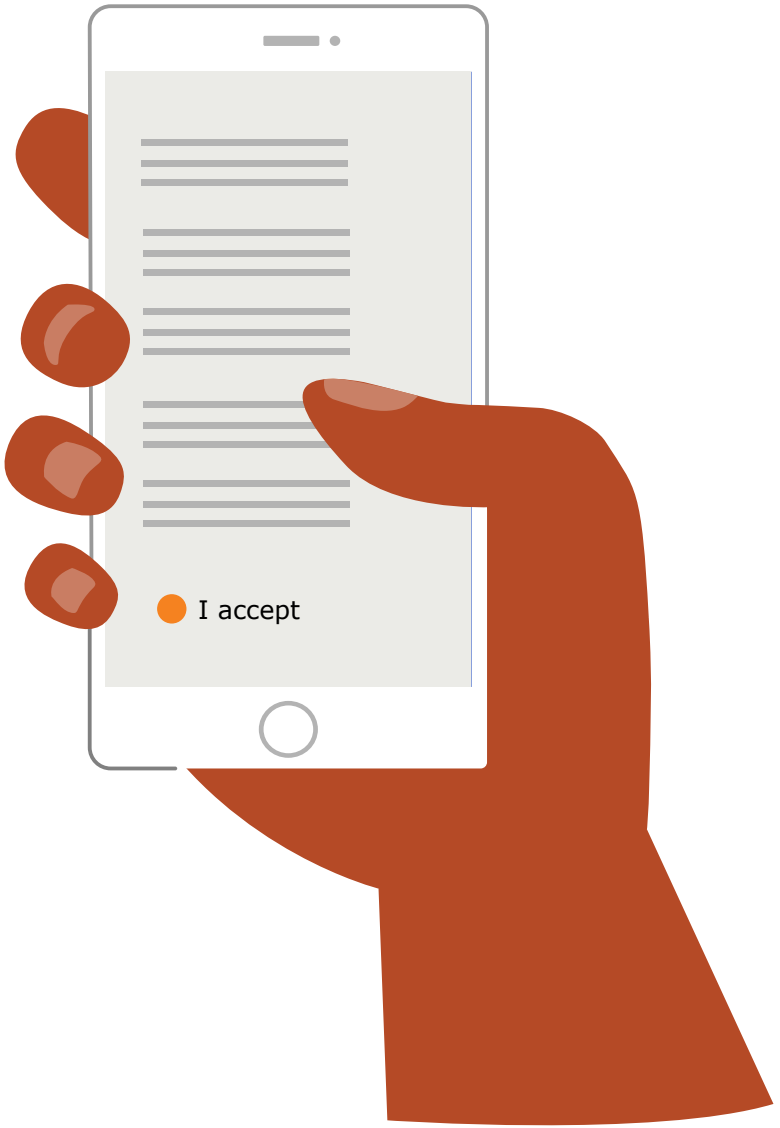
MEDIC helps innovators and entrepreneurs fill in knowledge gaps on the path to commercialization of their healthcare technology products. MEDIC conducts digital health applied research, provides advanced skill development services, and leads the design, development and testing of electronic medical records (EMR) systems, patient health records (PHR) systems, clinical assessment tools, and patient-facing mobile and web application development and device integration.

Clicking “I accept” is just not enough

Consumers should not need to choose between protecting their privacy and accessing valuable health information. Digital healthcare application developers should not have to decide either.

Healthcare data privacy must be respected and protected.

Digital healthcare services must adhere to a web of complex provincial, federal and international healthcare data privacy regulations. That complex regulatory environment can be difficult for healthcare entrepreneurs to navigate and implement. Here’s how to implement them and how to use them as a tool for navigating privacy and consent.



The Regulations

The regulatory landscape for personal health information and the protection of data is constantly changing.

The nature of digital healthcare technologies is global in scope, so it can be initially intimidating for developers to deal with the multijurisdictional nature of healthcare data privacy legislation. However, for every regulatory requirement, there are also legislative tools and policies that make the landscape easier to navigate.

According to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), it is the responsibility of the transferring organization to ensure that the receiving organization provides a level of protection to the personal information that is comparable to Canadian law. This can be accomplished through respecting the receiving jurisdiction's regulations — as long as they are as least as strict as Canada's — or through contract terms.

Here are the mechanisms and tools that make the system easier to navigate.

> I feel bad for companies that are hacked. However, if you don't have the appropriate policies and practices around IT security to protect the information you have collected, hacks are inevitable.
>
> **– Thomas White**

Thomas White is the eHealth Technology Project Lead at Mohawk College's MEDIC.

At the federal level, the PIPEDA defines the national privacy rules for the collection, use and disclosure of personal information, including health information as it relates to commercial activities.

At the provincial level in Ontario, look to the Personal Health Information Protection Act (PHIPA). There are equivalent pieces of legislation in other provinces. PHIPA outlines privacy rules that are specific to health information custodians (HIC). These rules cover individuals and organizations who receive personal health information from health information custodians.

When working with international partners, especially when personal health information is transferred outside of Canada by a government agency or a private organization, the laws of the country to which the information will be transferred apply. For Canadian innovators the US legislation related to HIPAA will be particularly relevant.

Jurisdictions and organizations across Canada are working to rationalize and streamline Data Sharing Agreements (DSA's) and the associated processes. Some have developed agreement frameworks which bring a variety of agreements together. A number of jurisdictions are also using a master agreement which includes core principles and obligations that is signed by all parties

Global context

There are also some unique features from international regulations that Canadian companies can consider adopting. They don't contradict Canadian regulations as they demand higher standards in terms of health data protection.

1 The European Union Data Protection Directive (EUDPD) requires that the collection and processing of personal health information must follow four standards: purpose limitation, data minimization, proportionality, and control.

2 The EU General Data Protection Requirement (GDPR) specifies that user consent must be acquired before data collection starts. Consent cannot be implied and user must be made implicitly aware of what they are consenting to, as well as the consequences if they do not consent to having their data used. Additionally, users have the right to request access to their data within 30 days.

Structuring a Privacy Agreement and Terms of Service

When accessing digital healthcare services, consumer see two documents on the tools they use: The Privacy Agreement and Terms of Service.

Here is what you need to know about creating privacy-focused documents.

With respect to the regulations, there are some specific issues that must be addressed in these agreements.

First and foremost, accredited legal advice on consumer consent must be obtained in all cases. This advice will outline the liabilities and limits on liabilities in providing direct-to-consumer healthcare services.

In a field with such a clearly articulated list of consumer rights, users cannot just scroll to the bottom of a privacy agreement or TOS and click "I accept," especially when working within an international agreement. Users might, for example, need to read and accept each clause individually. Double verification on more than one device or using unique text codes might need to be enabled.

From within any startup's legal position, the following seven regulatory points must be respected at every stage of the Privacy Agreement and Terms of Service creation process.

1 **Individuals have the right to know how their personal health information is being collected, used and disclosed.**

In general, the information submitted by the user can only be used to provide the service the user has requested. The service provider is responsible for ensuring their employees and partners comply with this requirement.

---

2 **Individuals have the right to access their Personal Health Information (PHI).**

This assumes that the records of the information concern only the individual who has accessed the digital healthcare service and their minor children.

3 **Individuals can withdraw their consent.**

One of the reasons consent must be direct, not implied, is that users who have accessed a digital healthcare service can withdraw their consent for the company to use their data at any time within a reasonable time frame.

---

4 **Individuals have the right to know what their data is being used for.**

The healthcare data submitted by users of the digital healthcare service can be used only for the delivery of the service itself. It cannot be used for marketing purposes, business intelligence purposes or to fulfill any other business need.

---

5 **In some jurisdictions, individuals have the right to request their data be destroyed.**

For a myriad of reasons, digital healthcare service consumers may ask for the removal of their data from the system and, in some cases, they may request that this data be destroyed without leaving a digital footprint.

---

6 **Consent is required for any use of individual's health information.**

The consent must be expressed through specific documentation, created by working with an accredited legal advisor.

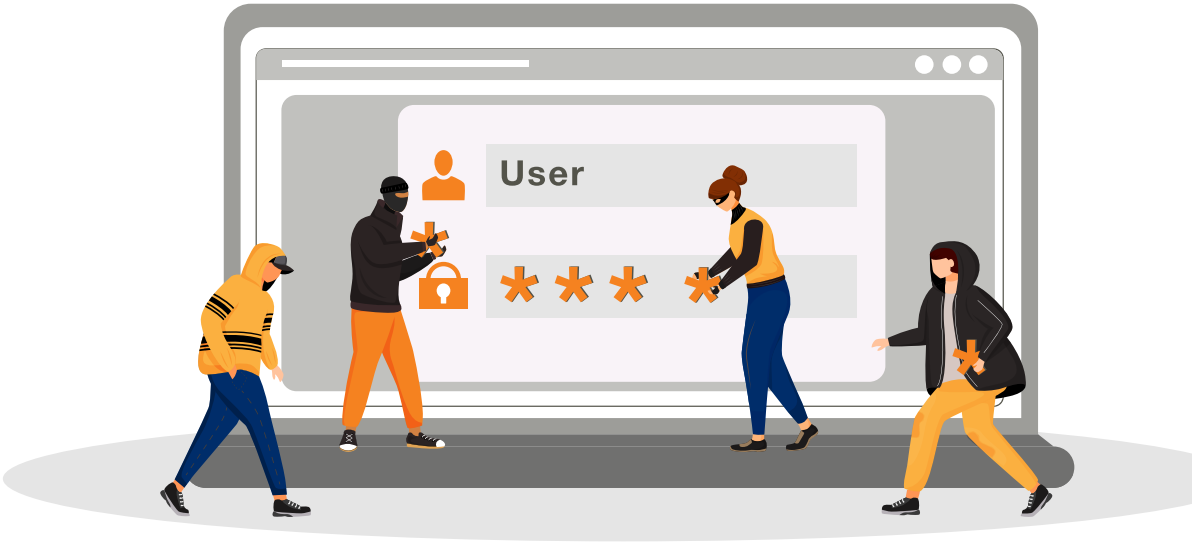
---

7 **Consent may not be required for research, provided that specific requirements and conditions are met, including ensuring data is anonymized.**

Any information that identifies the individual, or could be used to identify the individual by itself or in combination with other information, must be removed. The researcher or research team must work with the appropriate research ethics board and the Healthcare Information Custodian to ensure all regulatory requirements are met.

Understanding the role of the Healthcare Information Custodian (HIC)

One of the unique features of a digital healthcare privacy agreement is that it is under a kind of guardianship. Healthcare Information Custodians (HICs) fulfill the guardianship role, defined by PHIPA, of ensuring that rules for the collection, use, storage, disclosure and even disposal of healthcare data are set and followed. In fact, one of the terms of compliance is the appointment of an HIC. Ordinarily, this role is fulfilled by a healthcare practitioner working at a healthcare facility or medical practice. Independent consultants can also work as HICs for organizations that don't provide healthcare, but do collect healthcare information.



If there is ever a security breach that affects the privacy of personal health information, the HIC must be informed immediately. In turn, the HIC must make the information about the breach available to the public and any agency whose policies and regulations apply. The HIC is also responsible for describing implemented data protection safeguards and for ensuring that regular threat risk assessments and privacy impact assessments are conducted. They will also ensure agreements you have with employees or any other third parties comply with data disclosure restrictions and regulatory conditions. Whether the HIC is in-house, or retained through a third-party consultancy, they are caretakers of all the administrative, technical and physical safeguards required by regulations and corporate agreements with their users.

Storing data and security measures

Consent in data collection and the secure storage of that data demands some philosophical reckoning on the part of app developers. Before data is collected or stored, two questions need to be asked and answered.

- Does this data need to be collected and, if so, why?
- Does this data need to be stored and, if so, why?

In many ways healthcare technologies have to be implemented in ways that are contrary to the prevailing culture of other technology companies because of data privacy concerns. While many other tech companies are trying to break down departmental silos to enable better data sharing and insight communication, that is not possible when dealing with healthcare data that is shared with consent for a single purpose. Big data taxonomies that enable data scientists to capture every possible data point, without being certain as to how the data may be used, is not an ethos healthcare tech developers can embrace. In short, unlike other technology service providers, providers of healthcare technologies cannot collect consumer healthcare data and use it to build business intelligence to inform sales and marketing.

Does this data need to be collected and, if so, why?

Does this data need to be stored and, if so, why?

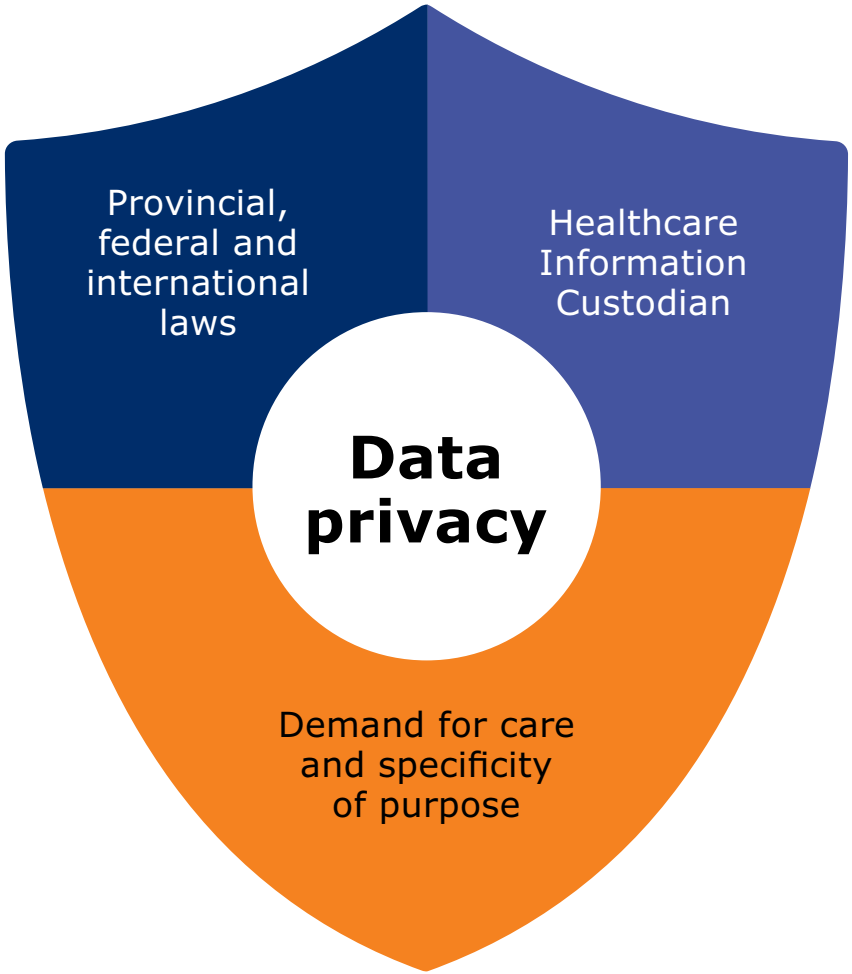
Technical specifications

There are many technical specifications to consider in order to be compliant with the different privacy legislations in terms of data storage. These include differences in hosting providers, and knowing what comes straight out of the box, and what needs to be configured. Health regulation compliance requires storage solutions to cover Physical, Technical, and Administrative safeguards. Choosing a cloud hosting provider that supports healthcare regulation compliance generally fulfills physical safeguard requirements. However, full compliance requires the business to adhere to strict technical and administrative safeguards.

Confidence in safeguards

Healthcare data privacy and consent may be complex issues to untangle, but each strand reveals another method to protect against both hackers and human error. Provincial, federal and international laws all demand respect for individual healthcare data. Coupled with that respect is a demand for care and specificity of purpose in the collection, storage, movement and even destruction of healthcare data. The third level of data care, the role of Healthcare Information Custodian, works toward ensuring that the laws are interpreted correctly and data protected using appropriate technology.

Clearly, a broader understanding of those three forces of data privacy care at the app development level can improve healthcare data privacy and security from the foundation upwards. As complex as the regulatory atmosphere may be, achieving an understanding of it is one more necessary step on the long path from concept to prototype to commercialization of healthcare apps.



Acknowledgements

This white paper was adapted from an applied research report prepared by Andrew Norgate, Tom White and Garrett Tyler of MEDIC.

mohawkcollege.ca/medic

ideaworks@mohawkcollege.ca

mohawk

IDEAWORKS

mHEALTH & eHEALTH DEVELOPMENT
AND INNOVATION CENTRE